Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

070.207 E-mail Distribution Lists

Version 2.2
December 15, 2017

Revision History

Date	Version	Description	Author
9/1/2002	1.0	Effective Date	CHFS IT Policies Team Charter
12/15/2017	2.2	Revision Date	CHFS OATS Policy Charter Team
12/15/2017	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

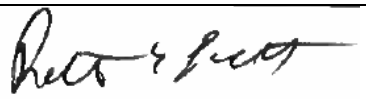
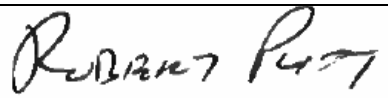
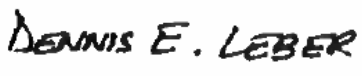
Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	12/15/2017		
CHFS Chief Security Officer (or designee)	12/15/2017		

Table of Contents

070.207 E-mail Distribution Lists

Category: 070.000 Administrative

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must implement an acceptable level of security controls to through an e-mail distribution policy. This document establishes the agency's E-mail Distribution Lists Policy to manage risks and provide guidelines for security best practices regarding lists created for information distribution through e-mail.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) to request an exception to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the CHFS OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3 Policy Requirements

3.1 General

The Cabinet for Health and Family Services (CHFS) manages the use of Email Distribution lists as described in this policy. For the purposes of this policy, distribution lists are categorized into three groups:

- Cabinet
- Departmental
- User Defined

Distribution lists are set up and owned by the Commonwealth Office of Technology (COT). These lists should be requested though a CHFS Authorized Agency's IT or HR Services Contact, by sending a ticket into the Commonwealth Service Desk (CSD) (CommonwealthServiceDesk@ky.gov) for a Distribution List to be created, Once the distribution lists are created, regardless of category, they must have a designated owner (a CHFS Employee) who will be responsible to oversee the appropriate use of the list and to periodically review the list for accuracy.

Attachments should be avoided, if possible. Users should utilize links to shared sites to provide access to documents. Brevity is always encouraged. The owner can designate additional employees to have pre-approval access to the list.

CHFS OATS IS Team recommends that a confidentiality statement be included on cabinet, departmental, and user defined distribution lists as well as individual email communications below the user's signature line. Example of a confidentiality statement would include, but is not limited to:

- This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.

3.2 Requesting a New Distribution List

Requests must be approved by:

- Cabinet- Secretary's Office.
- Departmental- Commissioner's or Executive Directors Office.
- User owned lists- appropriate Branch Manager or Director whose employee will serve as the designated owner.

Once approved, requests for establishing an email distribution list should be forward to a CHFS Authorized Agency's IT or HR Services Contact, who can then submit the request to the CSD for processing.

Modifications the Active Directory (AD) user's accessibility of the list(s) can be updated by the designated owner of the distribution list.

4 Policy Definitions

- **Cabinet Level:** The purpose of these lists is to send out information or alerts pertinent to staff from all organizations within the Cabinet. Use of these lists is restricted to the Office of the Secretary, the Office Human Resources Management (OHRM), and OATS.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Departmental Level:** These distribution lists are used for communications directed at a single department or office within the Cabinet. A primary and alternate designated owner will be appointed by each Commissioner or Executive Director. This appointee will be responsible for ensuring the proper usage of the list and will periodically review the list for correctness.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **User Defined:** These lists may be used to correspond with a group of email users who may or may not be within a single Cabinet organizational unit. These groups are designed around a "business purpose" or "area of interest". Examples include groups such as timekeepers, wireless coordinators, personnel liaisons, EEO Coordinators, etc. These lists must be owned by a Cabinet employee who is a member of the list. The owner will be responsible to oversee the appropriate use of the list and to periodically review the list for accuracy.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Authorized Agency's IT or HR Services Contact
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-084- E-mail Review Request Policy
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-12 Revision 1, Introduction to Information Security (Draft)
- National institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information